

Statement for the Record of

CHARLES E. ALLEN

**Assistant Secretary for Intelligence and Analysis
Chief Intelligence Officer
Department of Homeland Security**

**“THE HOMELAND SECURITY INFORMATION NETWORK: AN UPDATE ON
DHS INFORMATION SHARING EFFORTS”**

**U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk
Assessment**

13 September 2006

Chairman Simmons, Ranking Member Lofgren, Members of the Subcommittee, I am pleased to appear today alongside Vice Admiral (Ret.) Roger Rufe, the Department's new Operations Director, whose 34 years of experience with the United States Coast Guard will prove invaluable in his new mission.

Thank you for inviting me to update you on the progress that the Department has made in strengthening intelligence and information sharing with state, local, and tribal authorities and the private sector through the Homeland Security Information Network (HSIN).

As the DHS Inspector General noted in his June 2006 report on HSIN, "State and local personnel have opportunities and capabilities not possessed by federal agencies to gather information on suspicious activities and terrorist threats. By working together, the various levels of government can maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks." The Homeland Security Act of 2002 gives the Secretary—broad responsibilities to access, receive, and integrate intelligence, law enforcement, and other information from state, local, and tribal government agencies and the private sector; and to disseminate to them, as appropriate, analysis to assist in the deterrence, prevention, and preemption of, or response to terrorist attacks against the United States. The Secretary has delegated these responsibilities to me as Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer.

DHS has a federal responsibility to develop and disseminate threat alerts, notifications, warnings, and threat-based risk assessments. The audience includes, but is by no means limited to, state and local officials, and other public safety entities; emergency fire and rescue services personnel; public health officials; transportation and coastal maritime security officials; and local government agencies supporting federal efforts to interdict illegal narcotics, alien, and other transnational trafficking activities. This is an important mission that I and the Department are firmly committed to fulfilling.

As vital as HSIN is to the fulfillment of this critical information sharing mission, I should remind you that HSIN is just one of the Department's ongoing efforts to enhance information sharing with our non-federal partners. The Office of Intelligence and Analysis has embraced a comprehensive series of initiatives to improve information sharing with our state, local, tribal, and private sector partners. For example, I have previously addressed before this Subcommittee one of this Department's most important initiatives, the State and Local Fusion Center (SLFC) Implementation Plan. Under this plan, which Secretary Chertoff approved on 7 June of this year, DHS ultimately will embed intelligence and operational personnel in SLFCs to facilitate the flow of timely, actionable, "all-hazard" information between and among state and local governments and the national intelligence and law enforcement communities, in support of the President's Guidelines for the Information Sharing Environment. These deployed professionals will form the basis of a nationwide homeland security information network for collaboration and information sharing. My Office is the executive agent for this Department-wide effort. Already we have placed intelligence personnel in fusion centers in Los Angeles, New York City, Maryland, Georgia, and Louisiana; we are pursuing an aggressive schedule to staff additional fusion centers across the country in accordance with their needs.

Additionally, in accordance with the December 2005 Presidential Guidelines and Requirements in Support of the Information Sharing Environment, we have been working closely both with the Office of the Program Manager for the Information Sharing Environment and the Department of Justice to develop a common framework for the sharing of terrorism and other threat-related information among executive departments and agencies and state and local entities, including law enforcement agencies. This framework ultimately will strengthen and codify relationships and permit the effective interface between the Intelligence Community and the emerging network of fusion centers. Most importantly, this framework will establish a process to ensure that the federal government speaks with "one voice" to state and local partners. Consistent with its authorities and mandate, the Department will coordinate with the Department of

Justice, NCTC and the FBI to ensure that all “federally coordinated” terrorism products are created for, and disseminated to, these partners.

Moreover, under my leadership as the Department’s Chief Intelligence Officer, we are developing, in coordination with the component agencies and the Chief Information Officer, an intelligence information architecture. This architecture will transform the decentralized and uncoordinated “as-is” state of the Department’s intelligence sharing infrastructure by identifying gaps in Department-wide capabilities and other areas where the management of information across the Department, and with our external partners, demands improvement. Through this architecture we will achieve a fully integrated intelligence information sharing enterprise. To implement this plan, we have formed a number of working groups to undertake specific tasks in analyzing requirements, conducting prototyping and piloting of emerging technologies, and initiating the acquisition of necessary capabilities. This effort represents a central thrust of our initiative to improve and optimize information flow both within the DHS intelligence enterprise and between this enterprise and our state and local partners.

Leveraging these additional information sharing efforts with a robust HSIN platform will optimize the ability of the Department to communicate critical information clearly, efficiently, and effectively both within DHS and among its many external partners. That said, the DHS Operations Directorate is HSIN’s institutional home, and I will let Vice Admiral Rufe speak to the overall efforts to strengthen and perfect HSIN. However, I want to share with you my Office’s initiatives to support information sharing using HSIN and other capabilities.

As I have stated, HSIN plays a major role within my Office’s intelligence information sharing program. My analysts, in coordination with the Department’s Office of State and Local Government Coordination, each of the Department’s operational components, other Federal agencies with homeland security functions, and the National Counterterrorism Center (NCTC), routinely post products to HSIN’s law enforcement, emergency management, international, and state and local intelligence communities.

The Department filled a vital near-term requirement and mandate by moving rapidly to establish network connectivity to all 50 States, many major cities, and five U.S. territories by December of 2004. However, significant time constraints encountered in meeting the ambitious roll-out plan did not permit DHS to do all that it would have ideally wanted to do before launching the system. Nevertheless, as the system has and continues to mature, the Department remains committed to improve its usefulness and accessibility.

Shortly after becoming Chief Intelligence Officer of DHS, my Office conducted a study on how we could improve the flow of Sensitive but Unclassified (SBU) intelligence information to the State and local environment. In November and December 2005, my staff also conducted a user requirements study, including a survey of state and local fusion centers, and used the results to develop a concept of operations and an interim governance structure for more effectively moving information between my Office and our state, local and private sector partners. Based on this we have implemented a pilot project to share unclassified intelligence information with and among the states using the existing HSIN platform—this project is known as HSIN-Intel.

The HSIN-Intel pilot project involves six states: Arizona, California, Florida, Illinois, New York, and Virginia. The participants include senior representatives from the intelligence offices supporting the Homeland Security Advisors, leadership and senior analysts of state and local fusion centers, and senior major urban area law enforcement executives from each of the respective states. The pilot governance structure is managed through a steering group of the participants, ensuring direct input from the participants into the development of the system. DHS Intelligence uses HSIN-Intel primarily to disseminate current homeland security intelligence information and integrated intelligence assessments derived both from DHS and Intelligence Community sources. DHS Intelligence personnel also are able to access, receive, and analyze law enforcement and intelligence information provided by the state and local partners; fuse this information with national intelligence and other information; and report threat information back to the State and local participants for action. Finally, through HSIN-

Intel, DHS Intelligence personnel are able to receive and promptly respond to state and local requests for assistance and information that are passed via the HSIN-Intel portal.

In addition to the “finished” intelligence products—that is, products which contain analytic assessments and which have been fully vetted—DHS Intelligence also provides through HSIN-Intel unevaluated, or “raw,” homeland security-related reporting, such as Homeland Intelligence Reports. In the first five months of the pilot operation, my Office has posted more than 500 documents on HSIN-Intel and the states have posted an additional several hundred.

We are taking steps in partnership with the Operations Directorate to continue to develop this pilot program in line with the approach that the Office of the Inspector General advocates in its June 2006 report. In fact, launching HSIN-Intel in its pilot form has given the Department the opportunity to “road-test” business processes and functional capabilities that could be used to further strengthen the larger HSIN enterprise. To that end, we have taken steps to ensure that any law enforcement or other sensitive homeland security related information shared throughout the HSIN-Intel portal is appropriately handled and that all parties understand and apply the rules in order to achieve the appropriate protections to their data.

Among its more immediate benefits, HSIN-Intel users have greater situational awareness of worldwide terrorism events. For instance, the day after the 11 July 2006, attacks on the transit system of Bombay, India, my Office transmitted relevant intelligence reporting, held a “quick-look” teleconference with all HSIN-Intel members, and was able to provide valuable information that was not already widely available to the public. We are looking forward to transitioning this program to full operational capability in the near term, and will continue to work directly in that regard with the customer based steering group and the Operations Directorate.

Whereas HSIN-Intel will continue to develop a robust capability for sharing and exchanging valuable and sensitive unclassified information, my Office also provides intelligence products up to the collateral SECRET classification level to our State and local partners through what is known as the HSIN-Secret network, or HSIN-S. Much like

the unclassified HSIN enterprise, HSIN-S also was developed within the Department to enhance rapid classified information sharing with State Homeland Security Advisors, emergency operations centers, state and local fusion centers, and major urban area police departments. Through HSIN-S, we are able to post directly both unclassified and classified threat products, such as Homeland Security Assessments, on systems accessible by many of our state and local partners. Since August 2005, my Office has posted more than 150 products on HSIN-S.

Secure connectivity to the states is essential for our collaboration, but HSIN-S's inherent limitations prevent us from going where we need to be in this regard. In recognition of this, we are aggressively moving to transition from HSIN-S to a more robust Secret-level classified communications network system—the Homeland Security Data Network (HSDN). HSDN is analogous to the Department of Defense's Secret Internet Protocol Network, or SIPRNET. With HSDN, government agencies are able to share information and collaborate in order to detect, deter and mitigate threats to the homeland at the Secret level. This new capability will enable our external state and local government and private sector partner with a Secret clearance to have information sharing collaboration capacity at that level. We have already begun to roll out HSDN to all state and local fusion centers. I intend to have HSDN installed everywhere I have officers assigned to a fusion center by the first quarter of Fiscal Year 2007. In the initial phases of its deployment, only DHS officers will have access, but we plan to expand access to appropriately cleared state and local personnel.

In conclusion, DHS Intelligence, like our colleagues in Admiral Rufe's Operations Directorate and the rest of the Department, takes seriously its obligation to partner with state, local, and tribal authorities and the private sector to share the information needed to protect our homeland. As a member of the Intelligence Community, my Office also is working closely with the Office of the Director of National Intelligence, the Office of the Program Manager for the Information Sharing Environment, the National Counterterrorism Center, the Department of Justice, the FBI, and others, to create efficiencies and interoperability among the existing intelligence information systems to enhance our collaborative efforts.

To prevent and counter potential terrorist attacks, first responders and front-line law enforcement officers must be armed with the information to recognize and defeat the threat. Similarly, the Department of Homeland Security must gain the insights of local law enforcement and emergency personnel as they identify trends and patterns involving potential threats to our Homeland. The networks we implement must serve this flow of information. I look forward to answering your questions.

###